УДК 681.03

АЛГЕБРАИЧЕСКИЙ ИММУНИТЕТ БУЛЕВЫХ ФУНКЦИЙ

М.Э. Тужилин

Российский государственный гуманитарный университет, г. Москва

E-mail: mtmt@rambler.ru

Сделан обзор публикаций, посвященных построению функций с максимально возможным алгебраическим иммунитетом.

Ключевые слова: *алгебраический иммунитет*, *булевы функции*, *алгебраическая атака*, *криптография.*

В [1] был предложен новый метод криптографического анализа фильтрующего генератора. Рассмотрена следующая задача. Предполагается, что известна функция усложнения f и характеристический многочлен линейной рекуррентной последовательности (ЛРП) $h(x)$, определяющие фильтрующий генератор. Требуется по отрезку выходной последовательности длины m определить ключ схемы – начальное заполнение генератора – $k_0, k_1, \ldots, k_{n-1}$. Задача сводится к решению системы уравнений вида

$$\begin{cases} b_0 = f(k_0, k_1, ..., k_{n-1}), \\ b_1 = f(L(k_0, k_1, ..., k_{n-1})), \\ ... \\ b_{m-1} = f(L^{m-1}(k_0, k_1, ..., k_{n-1})), \end{cases} \tag{1}$$

где L – линейная форма, определяемая многочленом $h(x)$.

Можно рассматривать аналогичную задачу и для необязательно последовательных знаков выходной последовательности.

Суть предложенного авторами метода, который они назвали «алгебраической атакой», заключается в следующем. Произвольное уравнение из системы (1) можно записать в виде

$$f(s) = b_t. \tag{2}$$

Степень нелинейности этого уравнения определяется степенью нелинейности функции f. Если для специально подобранной булевой функции g выполняется условие $d = \deg fg < \deg f$, то, умножив обе части уравнения (2) на g, мы получим, например, для $b_t = 0$ уравнение

$$f(s)g(s) = 0,$$

которое имеет степень нелинейности d.

В результате, если для функции f существует функция g с минимально возможным значением параметра d, то исходная задача может быть сведена к решению переопределенной системы уравнений, для решения которой разработан ряд методов (линеаризация, вычисление базиса Грёбнера, XSL-метод и т.д.).

В работе [2] алгебраическая атака получила новое развитие и новое название – «быстрая алгебраическая атака». Этот метод основан на существовании тождеств низкой степени, связывающих значения функции f и значения её аргументов $k_0, k_1, \ldots, k_{n-1}$.

Позднее появились и другие работы, в которых предложенный метод был улучшен и обобщён, например [3 – 5]. В работе [5] было продемонстрировано на реально существующей криптосистеме, как работает алгебраическая атака.

Естественно, появились работы, в которых предпринимались попытки разработать теорию противостояния предложенным методам.

В работе [6] было введено следующее понятие алгебраического иммунитета. *Алгебраическим иммунитетом AI(f) булевой функции f* называется минимальное значение d, такое, что существует булева функция g степени d, не равная тождественно 0, аннулирующая функцию g или её отрицание, то есть выполнено соотношение $fg = 0$ или соотношение $(f + 1)g = 0$.

Очевидно, что чем выше алгебраический иммунитет функции, тем сложнее применение алгебраической атаки к фильтрующему генератору, использующему выходную функцию f.

1. Основные понятия и обозначения теории булевых функций

Введем необходимые обозначения и напомним основные понятия теории булевых функций.

Множество булевых функций от n переменных обозначается через B_n. Носитель $\mathrm{supp}(f)$ булевой функции f определяется как множество $\{(x_1, \ldots, x_n) \mid f(x_1, \ldots, x_n) = 1\}$. Под весом Хемминга $\mathrm{wt}(f)$ булевой функции f понимается мощность $|\mathrm{supp}(f)|$. Равновероятной (или сбалансированной) называется булева функция, удов-

летворяющая условию $\mathrm{wt}(f) = 2^{n-1}$. Расстоянием Хемминга $d(f, g)$ между двумя булевыми функциями f и g называется величина $\mathrm{wt}(f \oplus g)$.

Любая булева функция f может быть однозначно представлена многочленом Жегалкина (алгебраической нормальной формой – *ANF*(*f*)). Число переменных в терме наивысшего порядка с ненулевым коэффициентом называется алгебраической степенью функции f и обозначается через $\deg(f)$. Мерой «удаленности» от множества A_n аффинных функций (то есть функций, для которых выполнено условие $\deg(f) \le 1$) является степень нелинейности булевой функции $nl(f) = \min\limits_{g \in A_n} d(f, g)$. Этот параметр может быть вычислен с помощью разложения Фурье функции f. Если разложение Фурье имеет вид

$$F_f(a) = \sum_{x \in GF(2)^n} (-1)^{f(x)+(x,a)},$$

то

$$nl(f) = 2^{n-1} - \frac{1}{2}\max\left|F_f(a)\right|.$$

2. Основные результаты об алгебраическом иммунитете

В [1] (точнее, в расширенном варианте работы, выложенном в Интернете) доказано, что для любой функции f справедлива оценка

$$AI(f) \le \left\lceil \frac{n}{2} \right\rceil.$$

В [7] доказано, что доля равновероятных функций от n переменных, для которых выполнены неравенства

$$\frac{n}{2} - \sqrt{\frac{n}{2}\ln n} \le AI(f) \le \frac{n+1}{2},$$

стремится к 1 при $n \to \infty$.

Обозначим через $B_{n,k}$ множество булевых функций от n переменных, имеющих алгебраический иммунитет, равный k. В [8] показано, что для всех значений k, удовлетворяющих условию

$$k \le \left\lceil \frac{n}{2} \right\rceil,$$

множество $B_{n,k}$ не пусто.

Очевидно, что

$$|B_{n,0}| = 2.$$

В [9] доказано равенство

$$\left|B_{n,1}\right| = 2 - 2^{n+1} + \sum_{m=1}^{2^n-1}\sum_{r=1}^{n} F_n(m, r)\cdot 2^{r+1}\cdot(2^{2^n-r}-1)\cdot(-1)^{m+1},$$

где $F_n(m, r) = \dfrac{f_n(m, r)}{m!}$, а $f_n(m, r)$ задается итеративно:

$$f_n(m, r) = \begin{cases} 0, & \text{если } r > m, \\ f_n(m-1, r)\cdot(2^r - m) + f_n(m-1, r-1)\cdot(2^n - 2^{r-1}), & \text{если } r \le m. \end{cases}$$

3. Построение функций с максимально возможным алгебраическим иммунитетом

Ряд работ посвящён построению классов булевых функций, имеющих максимально возможный алгебраический иммунитет, равный $\left\lceil \frac{n}{2} \right\rceil$. Существует несколько подходов к построению таких функций. Они обсуждаются в [10, 11].

Первый из них заключается в итеративном конструировании булевых функций от $2k$ переменных с алгебраическим иммунитетом, равным k. Впервые он был опубликован в [12].

Обозначим через φ_{2k} булеву функцию от $2k$ переменных, определенную рекурсивно:

$$\varphi_{2k+2} = \varphi_{2k} \,||\, \varphi_{2k} \,||\, \varphi_{2k} \,||\, \varphi^1_{2k},$$

где символ || обозначает конкатенацию таблиц истинности, а φ^1_{2k} определяется рекурсивно:

$$\varphi^i_{2j} = \varphi^{i-1}_{2j-2} \,||\, \varphi^i_{2j-2} \,||\, \varphi^i_{2j-2} \,||\, \varphi^{i+1}_{2j-2} \text{ для } j > 0,\ i > 0$$

и начальными условиями $\varphi^0_j = \varphi_j$ для $j > 0$, $\varphi^0_i = i \bmod 2$ для $i \ge 0$.

Доказано, что $AI(\varphi_{2k}) = k$.

Свойства построенных функций изучаются в [13]. Во-первых, там показано, что эти функции не равновероятны. Во-вторых, их алгебраические степени близки к $2k$, но степени нелинейности таких функций равны

$$2^{n-1} - \binom{n-1}{\frac{n}{2}},$$

то есть далеки от максимума.

Второй подход основан на модифицировании симметрических функций [11, 14]. Введем в рассмотрение функции следующего вида:

$$f(x_1, \ldots, x_{2k}) = \begin{cases} 0, \text{ если } \mathrm{wt}(x_1, \ldots, x_{2k}) \le k, \\ 1 - \text{в противном случае.} \end{cases}$$

Доказано, что функции от $2k + 1$ переменных вида $x_{2k+1} + f(x_1, \ldots, x_{2k})$ имеют алгебраический иммунитет $k + 1$ и что они равновероятны. Такой же алгебраический иммунитет имеют функции вида $x_{2k+2} + x_{2k+1} + f(x_1, \ldots, x_{2k})$.

Этот же подход к построению булевых функций с оптимальным значением алгебраического иммунитета был независимо предложен в [15].

Булевы функции от нечетного числа переменных рассматриваются также в [16].

Из [17] известно, что булева функция от нечетного числа переменных с максимальным алгебраическим иммунитетом всегда равновероятна. Авторами предложен метод построения функций от нечетного числа переменных с максимальным алгебраическим иммунитетом и высокой степенью нелинейности.

Важный частный случай исследован в [18]. Там представлена рекурсивная процедура построения всех симметрических булевых функций от 2^m переменных, имеющих максимально возможный алгебраический иммунитет, равный 2^{m-1}. Доказано, что число таких функций равно $3 \cdot 2^m$.

В [19] для произвольной булевой функции предложен метод доказательства того, что она имеет фиксированный алгебраический иммунитет. На его основе получен способ построения равновероятных функций от нечетного числа переменных с максимально возможным алгебраическим иммунитетом.

Этот метод обобщён в [20], и там построен новый класс равновероятных функций с максимально возможным алгебраическим иммунитетом.

4. Алгоритмы вычисления алгебраического иммунитета

Отметим, что вычисление алгебраического иммунитета для произвольной булевой функции – довольно сложная вычислительная задача. Поэтому ряд работ посвящён проблемам построения эффективных алгоритмов вычисления алгебраического иммунитета для булевых функций, заданных различными способами (в виде многочлена Жегалкина, в виде ДНФ, с помощью функции «след» и т. д.). Выделим работу [21], посвященную этой проблематике.

В [22] предложено два алгоритма нахождения алгебраического иммунитета S-боксов, построенных на основе степенного отображения.

В [23] получена классификация всех равновероятных функций от пяти переменных по отношению к алгебраическому иммунитету. Всего таких функций 601080390. В таблице приведено количество функций с заданным значением $AI(f)$ и их доля среди всех рассмотренных функций.

$AI(f)$	1	2	3
Число равновероятных функций	62	403315208	197765120
Доля от общего количества	10^{-7}	0,671	0,329

5. Новые направления исследований

Дальнейшее развитие рассматриваемая тематика исследований получила в двух направлениях, которые объединяет понимание того факта, что максимальный алгебраический иммунитет функции является необходимым, но недостаточным условием для гарантирования её высоких криптографических качеств.

Первое направление можно проиллюстрировать следующим примером. Пусть функция f имеет максимально возможный алгебраический иммунитет, равный $\left\lceil \frac{n}{2} \right\rceil$. Могут найтись функции g и h, удовлетворяющие свойству $fg = h$, причём $\deg h = \left\lceil \frac{n}{2} \right\rceil$, но $\deg g < \left\lceil \frac{n}{2} \right\rceil$. В этом случае низкая степень функции g может быть использована для построения быстрой алгебраической атаки, несмотря на максимальное значение $AI(f)$.

В [24] построено семейство равновероятных функций от четного числа n неизвестных с алгебраическим иммунитетом $n/2$, таких, что для функций f и g, удовлетворяющих условиям $fg = h$ и $\deg h = n/2$, выполнено условие $\deg g \geq n/2$.

Второе направление исследований связано с нахождением для оптимальных с точки зрения алгебраического иммунитета функций их алгебраической степени и степени нелинейности. Ведется поиск функций, значения всех параметров которых близки к оптимальным.

В [7] обсуждается связь между алгебраическим иммунитетом и степенью нелинейности функции. Доказана следующая оценка для произвольной булевой функции f с $AI(f) = k$:

$$nl(f) \geq 2^{n-1} - \sum_{i=k-1}^{n-k} \binom{n-1}{i} = 2\sum_{i=0}^{k-2} \binom{n-1}{i}.$$

В качестве следствия из неё для функций с максимальным значением $AI(f) = \left\lceil \frac{n}{2} \right\rceil$ получены следующие оценки.

Если n нечетно, то $nl(f) \geq 2^{n-1} - \binom{n-1}{\frac{n-1}{2}}$, если n четно, то $nl(f) \geq 2^{n-1} - \binom{n-1}{\frac{n}{2}}$.

В [10] построено несколько классов равновероятных функций с оптимальным значением $AI(f)$ и со степенями нелинейности, равными

$$2^{n-1} - \binom{n-1}{\frac{n}{2}-1} + 2\binom{n-2}{\frac{n}{2}-2}/(n-2) \text{ для четного } n$$

и

$$2^{n-1} - \binom{n-1}{\frac{n-1}{2}} + \Delta(n) \text{ для нечетного } n.$$

При этом $\Delta(n) = \begin{cases} 2\sum_{i=0}^{k-1} \binom{3k-2}{k+i-1} \frac{k-i}{k}, & n = 4k+1, \quad k \geq 4, \\ 2\sum_{i=0}^{k+1} \binom{3k-1}{k+i} \frac{k+2-i}{k+2}, & n = 4k+3, \quad k \geq 5 \end{cases}$

и $\Delta(15) = 268$, $\Delta(19) = 2436$.

Обсуждается там и вопрос об алгебраической степени построенных функций.

В [25] рассмотрены обобщения понятия алгебраического иммунитета на случай k-значных функций, заданных на конечном поле, введены понятия алгебраического иммунитета для блочного шифра и для поточного шифра, приведены оценки исследуемых параметров, указана связь этих параметров с вычислением базисов Грёбнера для ряда мономиальных упорядочиваний.

6. Связь между алгебраическим иммунитетом и нелинейностью *r*-го порядка

В [26] введено понятие профиля нелинейности булевой функции, то есть последовательности, r-й член которой равен степени нелинейности r-го порядка $nl_r(f)$, равной расстоянию функции f до класса функций, чья алгебраическая степень не превосходит r. В [27] получена нижняя оценка для параметра $nl_r(f)$ для функции f с $AI(f) = k$:

$$nl_r(f) \geq \sum_{i=0}^{k-r-1} \binom{n}{i} + \sum_{i=k-2r}^{k-r-1} \binom{n-r}{i} \tag{3}$$

и обсуждаются вопросы, связанные с применением данной характеристики булевой функции к криптоанализу.

В [28] применен новый подход к получению нижних оценок параметра $nl_r(f)$. Доказана теорема, следствием из которой является оценка (3). Для случая $r = 2$ эта оценка улучшена. Доказано, что для функции f с $AI(f) = k$ выполнено неравенство

$$nl_2(f) \geq \sum_{i=0}^{k-1} \binom{n}{i} + \sum_{i=0}^{k-1} 2^i \binom{n-2i-1}{k-1-i}.$$

Более того, показано, что эта оценка достижима.

Заключение

Рассмотренная проблематика, посвященная алгебраическому иммунитету булевых функций, уже выросла из первоначально возникшей задачи противодействия «алгебраической атаке». По-существу, на её базе возникла новая область исследования булевых функций. В последних публикациях на эту тему широко применяются алгебраические и комбинаторные подходы к получению оценок рассматриваемых параметров булевых функций, использующие характеры конечного поля, коды Рида – Малера и другие.

Постоянно растущее число публикаций и появление новых имен исследователей свидетельствуют о растущем интересе к данной проблематике и ее актуальности.

ЛИТЕРАТУРА

1. *Courtois N.*, *Meier W.* Algebraic Attacks on Stream Ciphers with Linear Feedback // Proceedings of Eurocrypt 2003, Lecture Notes in Computer Sciences. 2003. V. 2656. P. 345 – 359.
2. *Courtois N.* Fast Algebraic Attacks on Stream Ciphers with Linear Feedback // Proceedings of Crypto 2003, Lecture Notes in Computer Sciences. 2003. V. 2729. P. 176 – 194.
3. *Armknecht F.* Improving Fast Algebraic Attacks // Proceedings of FSE 2004, Lecture Notes in Computer Sciences. 2004 V. 3017. P. 65 – 82.
4. *Hawkes P.*, *Rose G.* Rewriting Variables: the Complexity of Fast Algebraic Attacks on Stream Ciphers // Proceedings of Crypto 2004, Lecture Notes in Computer Sciences. 2004. V. 3152. P. 390 – 406.
5. *Courtois N.* Cryptanalysis of SFINKS // Proceedings of ISICS 2005, Lecture Notes in Computer Sciences. 2005. V. 3935. P. 261 – 269.
6. *Meier W.*, *Pasalic E.*, *Carlet C.* Algebraic Attacks and Decomposition of Boolean Functions // Proceedings of Eurocrypt 2004, Lecture Notes in Computer Sciences. 2004. V. 3027. P. 474 – 491.
7. *Didier F.* A new upper bound of the block error probability after decoding over the erasure channel // IEEE Transactions On Information Theory. 2006. V. 52. No. 10. P. 4496 – 4503.
8. *Lobanov M.* Tight bound between nonlinearity and algebraic immunity // Cryptology ePrint Archive 2005/441.
9. *Tu Z.*, *Yingpu Deng Y.* Algebraic Immunity Hierarchy of Boolean Functions // Cryptology ePrint Archive 2007/259.
10. *Carlet C.*, *Zeng X.*, *Li C.*, *Hu L.* Further properties of several classes of Boolean functions with optimal algebraic immunity // Cryptology ePrint Archive 2007/370.
11. *Dalai D.*, *Maitra S.*, *Sarkar S.* Basic theory in construction of Boolean functions with maximum possible annihilator immunity // Designs, Codes and Cryptography. 2006. V. 40. No 1. P. 41 – 58.
12. *Dalai D.*, *Gupta K.*, *Maitra S.* Cryptographically significant Boolean functions: construction and analysis in terms of algebraic immunity // Proceedings of FSE 2005, Lecture Notes in Computer Sciences. 2005. V. 3557. P. 98 – 111.
13. *Carlet C.*, *Dalai D.*, *Gupta K.*, *Maitra S.* Algebraic immunity for cryptographically significant Boolean functions: analysis and construction // IEEE Transactions on Information Theory. 2006. V. 52. No. 7. P. 3105 – 3121.
14. *Braeken A.*, *Preneel B.* On the algebraic immunity of symmetric Boolean functions // Proceedings of Indocrypt 2005, Lecture Notes in Computer Sciences. 2005. V. 3797. P. 35 – 48.
15. *Armknecht F.*, *Krause M.* Constracting Single- and Multi-output Boolean Functions with Maximal Algebraic Immunity // Proceedings of ICALP 2006, Lecture Notes in Computer Sciences. 2006. V. 4052. P. 180 – 191.
16. *Li N.*, *Qi W.* Construction and analysis of Boolean functions of $2t+1$ variables with maximum algebraic immunity // Proceedings of Asiacrypt 2006, Lecture Notes in Computer Sciences. 2006. V. 4284. P. 84 – 98.
17. *Dalai D.*, *Gupta K.*, *Maitra S.* Results on algebraic immunity for cryptographically significant Boolean functions // Proceedings of Indocrypt 2004, Lecture Notes in Computer Sciences. 2004. V. 3348. P. 92 – 106.
18. *Liu F.*, *Feng K.* On the 2^m-variable Symmetric Boolean Functions with Maximum Algebraic Immunity 2^{m-1} // Proceedings of WCC. 2007. P. 225 – 232.
19. *Carlet C.* A method of construction of balanced functions with optimum algebraic immunity // Cryptology ePrint Archive 2006/149.
20. *Wang Y.*, *Fan S.*, *Han W.* New construction of Boolean function with optimum algebraic immunity // Cryptology ePrint Archive 2008/176.
21. *Баев В.В.* Эффективные алгоритмы получения оценок алгебраической иммунности булевых функций // Дис. ... канд. физ.-мат. наук. М.: МГУ им. М.В.Ломоносова, 2007.
22. *Nawaz Y.*, *Gupta K.*, *Gong G.* Efficient Techniques to Find Algebraic Immunity of S-boxes Based on Power Mappings // Proceedings of WCC. 2007. P. 237 – 246.
23. *Canteaut A.* Open problems related to algebraic attacks on stream ciphers // Proceedings of WCC 2005, Lecture Notes in Computer Science. 2006. V. 3969. P. 120 – 134.
24. *Dalai D.*, *Maitra S.* Balanced Boolean Functions with (more than) Maximum Algebraic Immunity // Proceedings of WCC. 2007. P. 99 – 108.
25. *Ars G.*, *Faugère J.* Algebraic Immunities of functions over finite fields // INRIA, Rapport de recherché №5532. 2005.
26. *Carlet C.* On the higher order nonlinearities of algebraic immune Boolean functions // Proceedings of Crypto 2006, Lecture Notes in Computer Science. 2006. V. 4117. P. 584 – 601.
27. *Mesnager S.* Improving the lower bound on the higher order nonlinearity of Boolean functions with prescribed algebraic immunity // Cryptology ePrint Archive 2007/117.
28. *Lobanov M.* Tight bounds between algebraic immunity and nonlinearities of high orders // Cryptology ePrint Archive 2007/444.